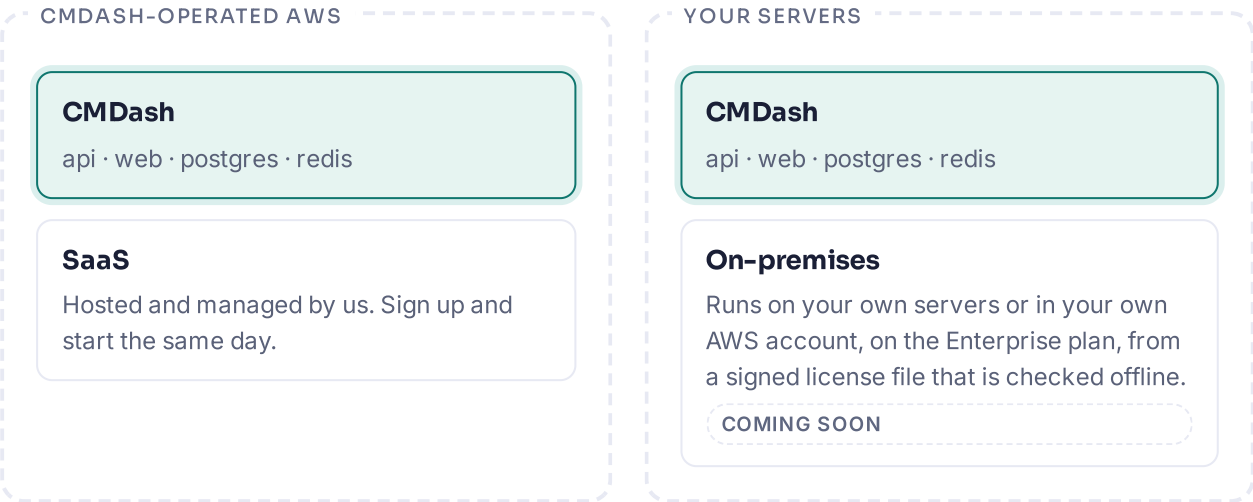


Architecture one-pager

What runs in production today: a managed, multi-tenant SaaS on AWS Lightsail in us-east-1, and how CMDash is deployed.

How CMDash is deployed



THE SAME PRODUCT IN BOTH · THE TRUST BOUNDARY IS WHAT CHANGES

What runs in production (7 components)

LAYER	COMPONENT	WHAT IT DOES
Edge	Amazon Route 53	DNS for cmdash.com and cmdash.net
	Lightsail load balancer	Terminates TLS with one certificate for the cmdash.net and cmdash.com hosts, redirects HTTP to HTTPS, and spreads requests across the instances
Compute	2 Lightsail instances	Each runs the same Docker Compose stack: a Caddy reverse proxy, the API (NestJS), the web app, the marketing site and customer portal, the staff admin app and the policy portal (Next.js), an update agent, and Redis

LAYER	COMPONENT	WHAT IT DOES
Data	Lightsail managed PostgreSQL 16	All tenant data, isolated by row-level security forced at the database, with automated daily snapshots and point-in-time restore
Storage	Amazon S3	Evidence files and generated reports, encrypted at rest with S3-managed keys (SSE-S3, AES-256)
Secrets	AWS Secrets Manager	The database credential and the JWT secret, read by the instances at boot
Control plane	1 Lightsail instance and its own managed PostgreSQL database	Accounts and licensing at api.cmdash.com, kept apart from the tenant data plane

This inventory is parsed from the architecture document in the CMDash repository. That document also describes a target architecture that has not been deployed, so it is not shown here.

Review the architecture with your own team

Start a 30-day free trial.

Or bring this inventory straight to your infra review.